REMARKS

In response to the Office Action mailed May 5, 2003, Applicant respectfully requests reconsideration. To further the prosecution of this application, each of the issues raised in the Office Action is addressed herein.

Initially, Applicant notes that the Office Action considers claims 1-32 as having been examined and pending in this application. However, Applicant canceled claim 28 in a preliminary amendment sent via facsimile on February 24, 2003. Accordingly, claims 1-27 and 29-32 are pending in this application, of which claims 1, 15 and 21 are independent claims.

I. Rejection Under 35 U.S.C. §103

In the Office Action, all of the claims (including independent claims 1, 15 and 21) are rejected under 35 U.S.C. 103(a) as purportedly being obvious over Ericson (U.S. Patent No. 6,061,753) in view of Yu (U.S. Patent No. 4,919,545). This rejection is respectfully traversed.

A. There is No Motivation to Combine Ericson and Yu

The Office Action concedes that Ericson does not disclose "authenticating the request at the storage system to authenticate the device issuing the request." (Page 3, ¶2 of the Office Action). However, the Office Action asserts that Yu discloses a security method for authorizing access to a resource and that it would have been obvious to one skilled in the art to "combine the teaching of Yu with the storage system of Ericson because it would have enable (sic) secure access to the storage system over a network." (Page 3, ¶2 of the Office Action). Applicant respectfully disagrees.

The Office Action does not point to any teaching in Ericson to suggest that the disclosed system is one wherein hosts are untrusted. Absent such a teaching, one skilled in the art would not have been motivated to complicate the system by employing authentication techniques, because they are not necessary.

Furthermore, not only is Ericson silent about an untrusted environment, but Ericson explicitly teaches a system for use in a trusted environment. The controlled data storage access system of Ericson is performed in a SCSI environment where initiators are trusted. Both the nature of the SCSI environment and the details of the SCSI interface make it unnecessary and therefore undesirable to implement verification or authentication methods as disclosed by Yu.

The SCSI protocol defines a standard for communication between a computer and various peripheral devices. In particular, various host devices (referred to as initiators) may issue requests to one or more peripheral devices (referred to as targets) that are connected to the SCSI bus. Each device (i.e., an initiator or a target) has a unique SCSI ID which identifies its physical location on the SCSI bus. The narrow SCSI bus and associated connectors support a maximum of eight devices. The wide SCSI bus and associated connectors support a maximum of 16 devices. See e.g., http://www.infran.ru/TechInfo/BSD/handbook114.html; http://scsifaq.paralan.com/.

The SCSI environment is local and contained, and therefore trusted and secure. Only a limited number of devices can be attached to a SCSI bus over a limited and local area. For example, internal SCSI connections (i.e., SCSI ribbon connections) are designed for communication between components and peripherals within the same computer (e.g., a personal computer). See e.g., http://computer.howstuffworks.com/scsi5.htm. External SCSI connections (i.e., SCSI cables) are designed to connect peripherals over relatively short distances. For example, SCSI cables typically come in 3ft and 6ft lengths. Although the cables may be daisy-chained, the SCSI protocol itself does not support bus lengths greater than 25 meters. Accordingly, a SCSI network is limited to a small area and limited to a small number of devices. See e.g., http://www.ramelectronics.net/html/scsi_connecters.html#cablelength.

In addition, each device on the SCSI bus must be manually configured and physically connected to the bus via an appropriate SCSI connector, and assigned a unique SCSI ID (often by manually setting a physical switch or configuring external jumpers). To assign a unique SCSI ID to a device (i.e., 0-7 for narrow SCSI and 0-15 for wide SCSI), the SCSI ID of every other device on the bus must be known to avoid conflicts. See e.g., http://computer.howstuffworks.com/scsi3.htm; http://www.seagate.com/support/kb/tape/w4m_scsi.html; http://support.gateway.com/s/CDROM/Panasonc/CS006aa/PANAS100.shtml.

Accordingly, there are no unknown or untrusted devices connected to a SCSI bus. An operator or administrator building a SCSI network must physically attach each device to the bus and configure it appropriately. http://www.sun.com/solutions/blueprints/0800/scsi.pdf (see especially "SCSI Issues in Clusters" on page 3, *et. seq.*) Therefore, the operator is cognizant of each device on the network and is fully in control of what devices are connected to the SCSI bus.

That is, untrusted devices cannot gain access to the SCSI bus. In such a local and trusted environment, it would have been unnecessary to implement verification and/or authentification procedures.

Furthermore, the SCSI interface itself prevents a device from misrepresenting its identity. The SCSI ID assigned to each device connected to a SCSI bus both identifies the device and specifies the device's physical address on the bus. The uniqueness of a SCSI ID is a requirement of the interface. http://www.sun.com/solutions/blueprints/0800/scsi.pdf. For example, bus arbitration and communication depends on each attached device having a unique SCSI ID. Conflicts with SCSI IDs prevent the conflicting devices from gaining access and communicating over the SCSI bus (and may result in the failure of all devices on the SCSI bus). http://www.ba-stuttgart.de/~schulte/htme/ebuss12.htm#REF2.1.2. The uniqueness of a device's SCSI ID is its license to access the bus. For a device to communicate over the bus, it must represent itself by that unique SCSI ID. Accordingly, there is no way for a device to misrepresent itself without disrupting the SCSI network. http://www.infran.ru/TechInfo/BSD/handbook115.html#210.

In Ericson, a plurality of initiators 100 are connected via a SCSI bus 104 to a target device 102 such as a disk array having a controller 106 (col. 3, line 53 – col. 4, line 5). Upon request by an initiator, the controller accesses a look-up data structure that defines which intiators have access to which logical units of the disk array to ensure that the request is permitted (col. 4, lines 6-54). It should be appreciated that allocation of logical units to particular initiators is conducted in a trusted environment. For example, column 4, lines 54-61 states:

> The look-up data structure may be pre-configured by a system operator who assigns selected logical units 108 in the target 102 to each of the initiators 100. This preconfiguration preferably is performed when the target controller 106 is installed. When necessary, however, the look-up data structure may be reconfigured at any subsequent time, such as when new initiators 100 are added to the system, or when the logical units 108 must be reassigned to other initiators 100.

The system operator configures the look-up data structure according to the devices on the SCSI bus and allocates logical units to new devices added onto the SCSI bus as desired. The system operator is trusted with properly adding devices to the SCSI bus and defining the look-up data structure to permit access as desired by associating initiator IDs with desired logical units.

In a SCSI environment, the system operator must give each device a unique SCSI ID which must remain unique in order for a device to communicate on the bus.

In this environment, there is no opportunity for a device to misrepresent its identity to gain access to restricted logical units of the target device. Accordingly, authenticating the identity of a device is completely unnecessary. While Ericson mentions that other peripheral interfaces may be used, Ericson does not contemplate untrusted environments or anywhere suggest that the described access method could be used in environments where there is a possibility that initiators may attempt to misrepresent their identity to gain access to restricted logical units.

Accordingly, one skilled in the art would not have been motivated by Yu to implement verification procedures in Ericson since those procedures would not have added any additional security and would have unnecessarily complicated the Ericson system without benefit. As such, the Office Action has failed to establish a *prima facie* case of obviousness and the rejection is therefore improper. Applicant respectfully requests that the rejection be withdrawn.

CONCLUSION

In view of the foregoing amendments and remarks, this application should now be in condition for allowance. A notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below to discuss any outstanding issues relating to the allowability of the application.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Respectfully submitted,
Steven M. Blumenau et al., Applicant

By: Richard Giunta

Richard F. Giunta, Reg. No. 36,149
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, Massachusetts 02210-2211
Telephone: (617) 720-3500

Docket No.E00295.70066.US
Date: August 4, 2003
x08/02/03